Maryland Cybersecurity Authority to Operate Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose

The State of Maryland Department of Information Technology (DoIT) is responsible for, and committed to managing the confidentiality, integrity, and availability of State government information technology (IT) networks, systems, and applications within the scope of its authority. This includes ensuring that all devices and networks comply with security policies and configuration standards before they are approved to operate in agency IT environments. This policy defines the requirements for granting an **Authority to Operate (ATO)** or **Interim Authority to Operate (IATO)** certification to an information system.

2.0 Document and Revision History

This policy supersedes the Maryland Information Security Policy v3.1 (2013), Section 5.1: Security Assessment and Authorization and any related policy regarding ATO/IATO declared prior to the 2017 Cybersecurity Program Policy. This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is applicable to all IT environments and assets utilized by any agency supported by, or under the policy authority of, the Maryland Department of Information Technology. DoIT will be responsible for determining whether or not devices are authorized to operate and for ensuring the authorization state of all such devices and networks for onboarded Agencies is being tracked.

Agencies under the policy authority, but not under direct management of DoIT, must independently comply with the requirements of this policy.

4.0 Policy

This policy includes the following requirements.

#	Name	Requirement
A	ATO / IATO Requirement	No new device, network, or application (collectively referred to as "information systems and connections") shall be permitted to operate without a risk assessment and a signed ATO or IATO form. ▪ Agencies with information systems and connections not currently under an ATO must be brought into compliance within one year of this policy's original publication date by providing a baseline ATO which verifies that security controls have been adequately implemented (or plan to be implemented) to protect confidential information and agree to accept the risk associated with the system. ▪ Compliance should be generally prioritized, with assets rated at Moderate or High security categories taking precedence over assets designated as Low security.

B	Approval Authority	All agencies shall identify a staff member as the **Designated Approval Authority (DAA)** for ATO/IATO decisions. This staff member will have the authority to sign (grant) an ATO/IATO for agency IT environments. This person may be the: ▪ Agency's Deputy CIO; or ▪ Director of Cybersecurity/State CISO or designated official (if agency IT or security decisions are handled by DoIT)
C	ATO Time Period	ATO's are granted for a default time period of 3 years, after which a new **System Security Plan (SSP)** must be completed for the authorized entity, system, or connection.
D	IATO Time Period	IATO's may be granted for a maximum time period of 6 months.
E	ATO Criteria for Approval	▪ Information systems and connections subject to the requirements of this policy must be identified in the agency's SSP indicating the agency is compliant with DoIT policies and configuration standards; ▪ SSP must have been completed within the past 3 months; ▪ The DAA must accept the identified risks of the system operating in the agency environment; and ▪ The DAA must sign the ATO
F	IATO Criteria for Approval	▪ Information systems and connections subject to the requirements of this policy must be identified in the agency's SSP indicating areas of compliance and non-compliance with DoIT policies and configuration standards; ▪ SSP must have been completed within the past 3 months; ▪ The DAA must accept the identified risks of the system operating in the agency environment, and the additional risks posed by identified areas of non-compliance; and ▪ The DAA must sign the IATO
G	Forms	DoIT will create and provide ATO and IATO forms.
H	Tracking	The agency will track the ATO / IATO status of all devices, networks and applications.
I	Reporting	▪ Agencies must be able to report on ATO / IATO status for all information systems and connections upon request ▪ Agencies with expiring ATO / IATO will provide updated security control reports, renewal documentation, or termination forms to their respective DAA within the quarter preceding the expiration ▪ Agency DAAs must report ATO/IATO status updates to the State CISO after each quarterly review
J	New Device Deployments versus Configurations	In order to provide for potentially high volumes of devices being continuously deployed across the enterprise: ▪ ATOs or IATOs may be granted for an information system configuration standard that has been evaluated in an SSP, rather than to individual devices or applications. ▪ Additional devices or applications that are deployed in such a way that they conform to, or inherit, the configuration standard that has received an ATO or IATO, may be automatically granted the authority to operate under that ATO or IATO, so long as the devices were deployed in accordance with DoIT *Configuration Management Policy*

5.0 Exemptions

This policy is established for use within the DoIT Enterprise. If an exemption from this policy is required, an agency needs to submit a DoIT Policy Exemption Form and clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks and the agency's mitigation strategy associated with this exemption. If the agency can accept the risk, an exemption to this policy may be granted.

6.0 Policy Mandate and References

The Cybersecurity Program Policy mandates this policy. Related policies include:

- Third Party Interconnection Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Authority to Operate (ATO)	Authority granted to an information system, by a Designated Approving Authority (DAA), to be used in accordance with its intended purpose within agency IT environments. An ATO authorizes operation of a Business Product and explicitly accepts the risk to agency operations.
Designated Approval Authority (DAA)	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Responsible for signing Authority to Operate (ATO), Interim Authority to Operate (IATO), and associated Third-Party Interconnection Agreements.
Interim Authority to Operate (IATO)	Temporary authority granted to an information system to be used in accordance with its intended purpose within agency IT environments. IATOs are used to permit information systems to operate although non-compliant with some agency security policies or requirements, so long as the information system is brought into compliance within a designated time period.
System Security Plan (SSP)	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

8.0 Enforcement

The Maryland Department of Information Technology is responsible for ensuring the existence of ATOs or IATOs for Enterprise onboarded agencies. The DoIT Cybersecurity Program identifies the minimum requirements necessary to comply with the information security standards and guidelines provided within Cyber Security Program Policy and its supporting policies. Agencies not directly managed by DoIT must exercise due diligence and due care to comply with the minimum standards identified by the relevant DoIT policies.

If DoIT determines that an agency is not compliant with this policy or any supporting policy, the non-compliant agency will be given a sixty (60) day notice to become compliant or at least

provide DoIT a detailed plan to meet compliance within a reasonable time before the issue is reported to the Secretary of Information Technology. After which, the Secretary of Information Technology, or a designated authority, may extend a non-compliant agency's window of resolution or authorize a DoIT representative to limit or restrict an agency's access to external and internal communications (effectively shutting down connectivity) until such time the agency becomes compliant.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Devices or networks found to be in operation without an ATO or IATO, or found to be in violation of the terms under which the ATO or IATO were granted, may be subject to immediate deactivation or disconnection from other agency environments and third parties.